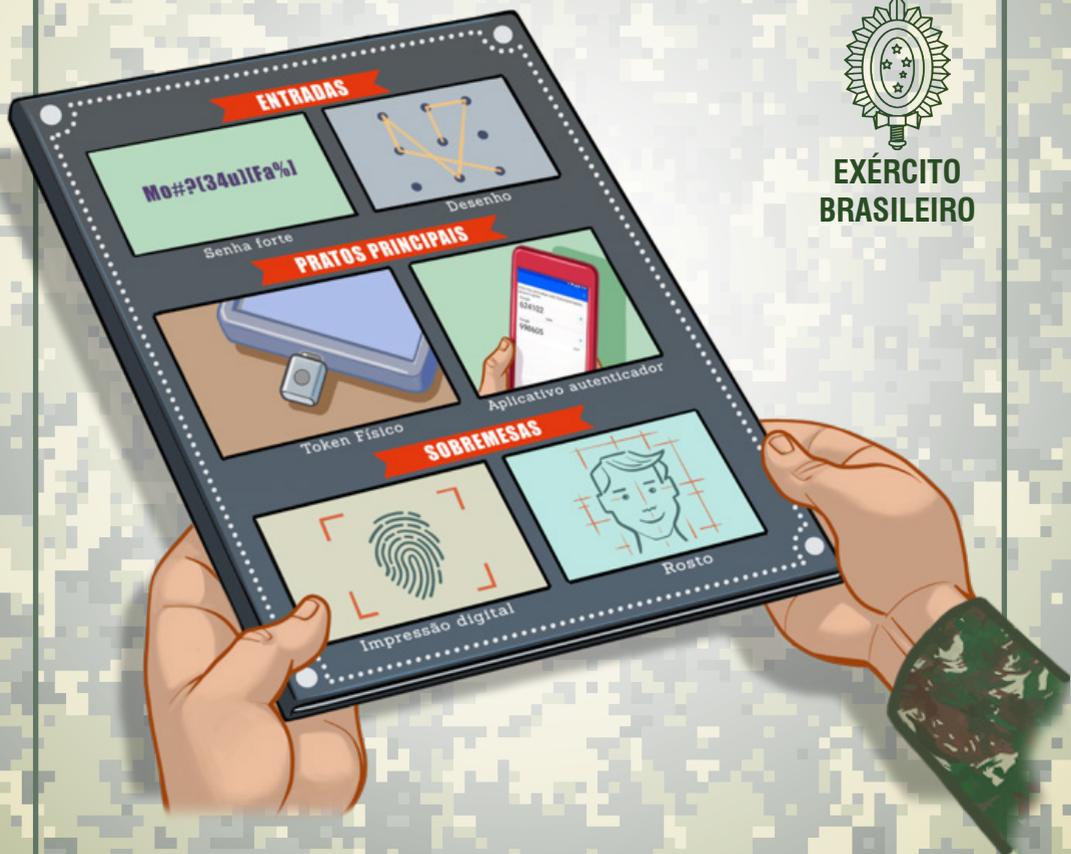
Campanha de Conscientização Cibernética
AUTENTICAÇÃO
ENTRADAS
Mo#?[34u][Fa%]
Senha forte
Desenho
PRATOS PRINCIPAIS
Token Físico
Aplicativo autenticador
SOBREMESAS
Impressão digital
Rosto
EXÉRCITO
BRASILEIRO
Produção:
COM D CIBER
E NA D CIBER

PROTEJA SUA VIDA DIGITAL: USE AUTENTICAÇÃO FORTE

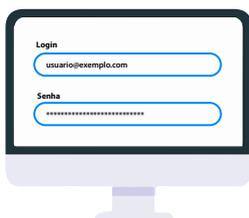
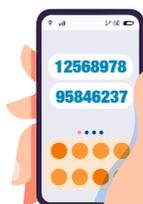
A autenticação ajuda a proteger o acesso às suas contas, evitando que alguém se passe por você. Mas com tantos ataques e vazamentos de dados, usar apenas senhas pode não ser proteção suficiente.
É preciso reforçar com uma segunda etapa de verificação.

Veja aqui os cuidados para deixar suas contas mais seguras.

CUIDADOS ESSENCIAIS PARA PROTEGER SUAS CONTAS

ATIVE A VERIFICAÇÃO EM DUAS ETAPAS

A verificação em duas etapas adiciona uma **segunda camada de proteção** no acesso às suas contas. Com ela ativada, mesmo que o atacante descubra sua senha, ele precisará de outras informações para invadir sua conta.

» Escolha o método que considerar mais prático e seguro, como:
- ter uma chave de segurança física
- usar um aplicativo de celular para gerar códigos de verificação
- receber códigos por mensagem de texto ou voz

Se o serviço não oferecer verificação em duas etapas, capriche ainda mais em seguir as próximas dicas, em especial as de **não reutilizar senhas**, criar senhas fortes e guardá-las de forma segura!

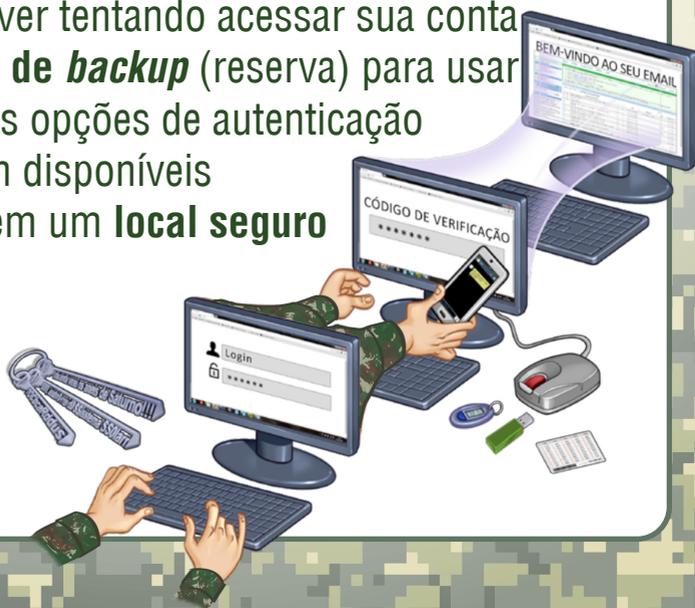
A chave de segurança física (ou token físico), também chamada chave U2F, FIDO ou FIDO2, é atualmente a opção mais segura de verificação. Alguns celulares mais modernos também permitem transformar o celular em chave física U2F/FIDO2.

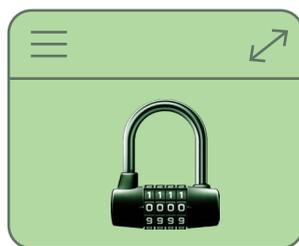
USE A VERIFICAÇÃO EM DUAS ETAPAS DE FORMA SEGURA

Para que a verificação em duas etapas realmente proteja suas contas, há algumas **dicas adicionais** que você deve seguir.

» Prefira chave de segurança física ou geradores de códigos de verificação por aplicativo de celular
  - use SMS apenas se não houver outras opções

» **Negue** toda requisição de autorização de login se você não estiver tentando acessar sua conta

» Gere **códigos de *backup*** (reserva) para usar quando outras opções de autenticação não estiverem disponíveis
  - guarde-os em um **local seguro**

USE UMA SENHA DIFERENTE PARA CADA CONTA

Reutilizar senhas, ou seja, usar a mesma senha em diversos lugares é arriscado, pois basta o atacante descobrir a senha de uma conta para conseguir acessar as demais contas onde ela é usada. Se desconfiar que uma senha usada em diversos lugares foi descoberta, **troque-a imediatamente** em todos os lugares em que é usada.

CRIE SENHAS FORTES

Se suas senhas forem **fáceis de serem descobertas** (fracas), suas contas de acesso e seus dispositivos podem ser facilmente **invadidos**.

» Crie senhas **longas**
  - escolha, por exemplo, três palavras aleatórias

» Adicione **diferentes caracteres**, para torná-las ainda mais fortes
  - misture números, caracteres especiais e letras maiúsculas e minúsculas

» Evite usar sequências de teclado

» **Não use** informações pessoais, como nomes, sobrenomes, datas e aquelas que você divulga em redes sociais

Está difícil lembrar de tantas senhas?
Veja a dica a seguir, sobre como guardá-las de forma segura!

GUARDE SUA SENHA DE FORMA SEGURA

São tantas senhas que é impossível guardá-las apenas de cabeça. Para ajudá-lo a não usar senhas fracas, adote o método de gerenciamento que considerar mais prático e seguro.

» Você pode, por exemplo:
  - usar aplicativos gerenciadores de senhas, ou
  - anotá-las em um papel e guardá-lo em local seguro, ou
  - gravá-las em um arquivo criptografado

ALTERE SENHAS EXPOSTAS EM VAZAMENTOS

Vazamentos de dados infelizmente ocorrem e suas senhas podem estar entre eles. Ao ficar sabendo que alguma senha sua foi exposta é importante **trocá-la imediatamente**.

» Fique atento a notícias sobre vazamentos de dados nos serviços que você usa

» Utilize os serviços de monitoramento de senhas, presentes em alguns sistemas e navegadores

SENHA

TENHA CUIDADOS ESPECIAIS COM CONTAS MAIS IMPORTANTES

Quanto mais “valiosa” sua conta, mais **atrativa** ela é para os atacantes. Por exemplo: a invasão de uma conta bancária pode acarretar prejuízos financeiros e, de uma conta de *e-mail*, pode levar à invasão de outras contas, se ela for usada para recuperação de senhas.

» Evite salvar senhas de contas importantes em ***navegadores web***, como as de acesso bancário, *e-mail* ou ID de sistema

» Não permita o ***login*** **automático** de contas importantes

NÃO COMPARTILHE SENHAS E CÓDIGOS DE VERIFICAÇÃO

Se conseguirem suas senhas e códigos de verificação, golpistas podem **invadir suas contas**, furtar sua identidade e praticar fraudes em seu nome, causando prejuízos a você e a seus contatos.

» Nunca repasse senhas ou códigos de verificação por mensagens, *e-mails* ou ligações

CONFIGURE SEUS EQUIPAMENTOS PARA EXIGIR AUTENTICAÇÃO NA TELA INICIAL

Equipamentos desbloqueados podem ser facilmente acessados por alguém, com acesso físico a eles.

» **Bloqueie** a tela do computador, *notebook*, *tablet* e celular, antes de sair de perto deles

» Configure seu celular e *tablet* para exigir atenção quando usar reconhecimento facial

» Ao usar **padrão de desbloqueio**:

- evite usar poucos pontos ou desenhos muito simples, como letras
- configure para o rastro ficar invisível

Padrão de desbloqueio é como são chamadas as senhas "desenhadas" na tela por meio da interligação de pontos.

ESCOLHA PERGUNTAS E DICAS DE SEGURANÇA DIFÍCEIS DE SEREM ADIVINHADAS

Perguntas e dicas de segurança são **recursos úteis** para ajudar você a se lembrar ou recuperar suas senhas, mas podem ser abusados por atacantes para invadir suas contas.

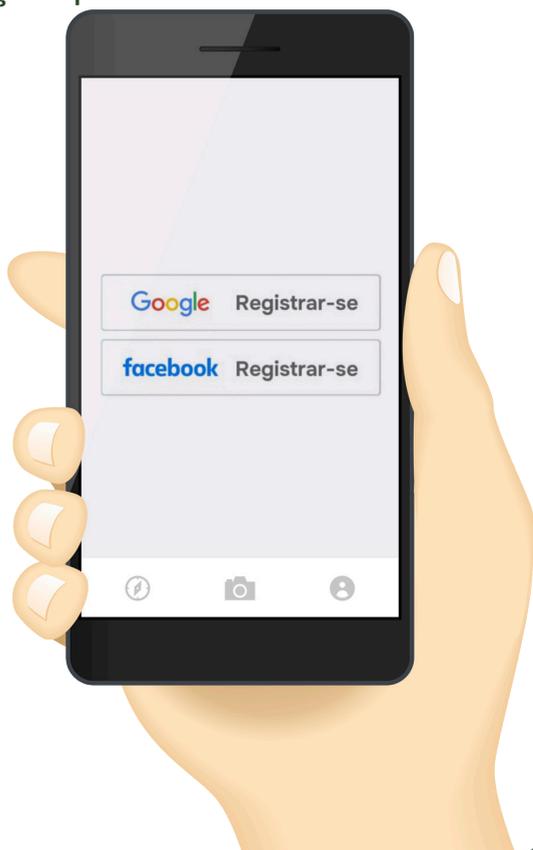
» Selecione perguntas de segurança cujas respostas sejam **difíceis de adivinhar**

» Escolha dicas de segurança vagas o suficiente para ninguém as descobrir e claras o bastante para você entendê-las

» Cadastre um ***e-mail* de recuperação** que você acesse regularmente, para não esquecer a senha desta conta também

REDOBRE OS CUIDADOS COM CONTAS USADAS COMO *LOGIN* SOCIAL

Alguns serviços permitem que você use uma **conta externa para se autenticar**, geralmente a da sua rede social ou serviço de *e-mail*. Ao centralizar seus acessos **em uma única conta**, se esta senha for exposta, todos os serviços que a usam estarão em risco.

» Verifique as opções oferecidas na conta usada como *login* social
- **restrinja** quais informações os serviços podem acessar
- elimine os acessos concedidos, se não forem mais necessários ou se desconfiar de ser um serviço malicioso

NÃO IGNORE OS AVISOS E ALERTAS DE LOGIN

Ficar atento aos **avisos e alertas** enviados pelos sistemas, de que houve tentativas de acesso às suas contas, ajuda a detectar usos indevidos.

» Observe as informações de **onde e quando** ocorreram os últimos acessos à sua conta e veja se realmente foram feitos por você

» Se perceber que sua conta foi indevidamente acessada:

- acesse-a diretamente, sem clicar em *links*
- altere a senha

» Ative imediatamente a **verificação em duas etapas** em suas contas, caso ainda não tenha feito

CUIDADO PARA NÃO COMPROMETER SUA SENHA

Para comprometer suas senhas, os atacantes podem observar você digitando, convencê-lo a abrir *links* maliciosos (*phishing*) ou infectar os equipamentos que você usa.

» Não abra todos os *links* e arquivos que recebe
- só leia códigos QR se confiar na fonte

» Mantenha seus equipamentos e aplicativos **atualizados**

» Evite digitar suas senhas em equipamentos de terceiros

» Use **conexões seguras**, como https para acessar sites

» Verifique se não há pessoas ou câmeras ao seu redor, enquanto você digita suas senhas

OUTROS CUIDADOS COM VERIFICAÇÃO EM DUAS ETAPAS

MANTENHA ATUALIZADOS OS DADOS USADOS NA VERIFICAÇÃO DE SUA IDENTIDADE

Alguns mecanismos de verificação baseiam-se em algo que apenas você tem para confirmar a sua identidade, como seu telefone celular. Isso pode se **tornar um problema** se seu telefone estiver indisponível ou você tiver trocado de número.

» Mantenha **atualizados** os dados para recebimento de códigos de verificação
» Cadastre *e-mails* e números de telefone **alternativos** para receber códigos de verificação, caso os principais estejam indisponíveis

CUIDADO PARA NÃO PERDER SEUS MECANISMOS DE AUTENTICAÇÃO

Se perder o mecanismo configurado como segundo fator de autenticação, outra pessoa pode usá-lo para **tentar se passar por você**.

- » Caso perca ou troque um dispositivo cadastrado como confiável, **exclua-o** nos serviços em que estiver configurado
- » Guarde sua chave de segurança física em um **local seguro**
    - caso a perca, avise imediatamente o serviço onde é usada
- » Revogue e **gere novamente** seus códigos de *backup*, caso os perca ou desconfie de que alguém os acessou

SAIBA MAIS
Para mais detalhes
sobre este e outros
assuntos relacionados
com cuidados na
Internet, consulte os
demais fascículos da
Campanha de
Conscientização
Cibernética no site
EB.MIL.BR

EXÉRCITO BRASILEIRO
Novos Desafios, Mesmos Valores

Produção: